

What is claimed is:

- 1 1. A system for detecting and deterring rollback attacks, comprising:
 - 2 a variable time period (VTP);
 - 3 a time duration to a next connection (TDNC);
 - 4 an access log;
 - 5 a server to transmit the variable time period (VTP) and the time duration
 - 6 to the next connection (TDNC) and to verify the access log; and
 - 7 a client to update the access log approximately every variable time period
 - 8 (VTP) and to connect to the server approximately after the time duration to the
 - 9 next connection (TDNC).
- 1 2. The system as recited in claim 1, wherein the client is a personal
- 2 computer (PC).
- 1 3. The system as recited in claim 1, wherein the client is a set-top box.
- 1 4. The system as recited in claim 1, wherein the server is a video home
- 2 server.
- 1 5. The system as recited in claim 1, wherein the server is a pay-per-view
- 2 video server.
- 1 6. The system as recited in claim 1, wherein the server is a video-on-
- 2 demand server.
- 1 7. The system as recited in claim 1, wherein the server is a media content
- 2 provider.
- 1 8. The system as recited in claim 1, wherein the next connection is a Secure
- 2 Authenticated Channel (SAC).

1 9. The system as recited in claim 1, wherein the access log is used for
2 billing.

1 10. A method for detecting and deterring rollback attacks, comprising:
2 establishing a shared secret between a client and a server;
3 transmitting, by the server to the client, a variable time period (VTP) and
4 a time duration to a next connection (TDNC);
5 updating, by the client, an access log approximately every variable time
6 period (VTP);
7 initiating, by the client to the server, a connection approximately after the
8 time duration to the next connection (TDNC);
9 transmitting, by the client to the server, the access log; and
10 verifying, by the server, the access log.

1 11. The method as recited in claim 10, further comprising:
2 establishing a new shared secret between the client and the server each
3 time the client connects to the server.

1 12. The method as recited in claim 10, further comprising:
2 establishing a new variable time period (VTP) and a new time duration to
3 a next connection (TDNC) each time the client connects to the server.

1 13. The method as recited in claim 10, further comprising:
2 incrementing, by the client, a counter, after each update to the access log.

1 14. The method as recited in claim 10, further comprising:
2 automatically detecting an anomaly.

1 15. The method as recited in claim 14, further comprising:
2 decreasing the variable time period (VTP), upon detecting an anomaly.

1 16. The method as recited in claim 14, further comprising:
2 decreasing the time duration to a next connection (TDNC), upon
3 detecting an anomaly.

1 17. The method as recited in claim 10, further comprising:
2 encrypting the access log.

1 18. The method as recited in claim 10, wherein each entry in the access log is
2 encrypted.

1 19. The method as recited in claim 10, wherein the access log is re-created,
2 each time the client connects to the server.

1 20. A machine for detecting and deterring rollback attacks, comprising:
2 a processor;
3 a storage device coupled to the processor;
4 a background component storable on the storage device and executable
5 on the processor to update an access log approximately every
6 variable time period (VTP); and
7 a content player component storable on the storage device and executable
8 on the processor to update the access log to indicate content
9 provided.

1 21. The machine recited in claim 20, wherein the background component is
2 capable of encrypting the access log.

1 22. The machine recited in claim 20, wherein the background component is
2 capable of encrypting each update to the access log.

1 23. The machine recited in claim 20, further comprising:
2 a communication component capable of connecting to a server
3 approximately after a time duration to a next connection (TDNC).

1 24. The machine recited in claim 23, wherein the communication component
2 is capable of transmitting the access log.

1 25. The machine recited in claim 23, wherein the communication component
2 is capable of receiving a new variable time period (VTP) and a new time
3 duration to the next connection (TDNC).

1 26. The machine recited in claim 20, wherein the communication component
2 is capable of receiving a new access log.

1 27. The machine recited in claim 26, wherein the background component is
2 capable of decrypting the new access log.

1 28. A machine-accessible medium having associated content capable of
2 directing the machine to perform a method of detecting and deterring rollback
3 attacks, the method comprising:
4 transmitting, by a server, a new access log; and
5 transmitting, by the server, a new variable time period (VTP) and a new
6 time duration to the next connection (TDNC).

1 29. The machine-accessible medium as recited in claim 28, wherein the
2 method further comprises:
3 receiving, by the server, an old access log; and
4 inspecting, by the server, the old access log.

1 30. The machine-accessible medium as recited in claim 28, wherein the
2 method further comprises:
3 establishing, by the server, a shared secret with a client;
4 decrypting, by the server, the access log;
5 encrypting, by the server, the new access log; and

6 encrypting, by the server, the new variable time period (VTP) and the
7 new time duration to the next connection (TDNC).

1 31. The machine-accessible medium as recited in claim 28, wherein the
2 method further comprises:

3 initiating, by a client, a connection with the server;
4 transmitting, by the client, the access log to the server;
5 receiving, by the client, the new access log;
6 receiving, by the client, the new variable time period (VTP) and the new
7 time duration to the next connection (TDNC); and
8 storing, by the client, the new access log, the new variable time period
9 (VTP), and the new time duration to the next connection (TDNC).

1 32. The machine-accessible medium as recited in claim 28, wherein the
2 method further comprises:

3 establishing, by a client, a shared secret with the server;
4 encrypting, by the client, the access log;
5 decrypting, by the client, the new access log; and
6 decrypting, by the client, the new variable time period (VTP) and the
7 new time duration to the next connection (TDNC).

1 33. The machine-accessible medium as recited in claim 28, wherein the
2 method further comprises:

3 updating, by a client, the new access log approximately every new
4 variable time period (VTP).